THAT WHICH IS CLAIMED:

1. A system for controlling installation of software, the system comprising:

an installation server, the installation server having access to first and second secret values associated with a copy of the software for installation;

an unencrypted installation client, the installation client incorporating the first secret value; and

an encrypted portion of the software, wherein the encrypted portion of the software is encrypted with a first key value derived from the first and second secret values; and

wherein the unencrypted installation client is configured to receive the second secret value from the installation server, to generate the first key value, to decrypt the encrypted portion of the software and to install the software.

2. A system according to Claim 1, wherein the installation client is further configured to generate a second key value from the first key value and the first secret value, encrypt the decrypted portion of the software with the second key value and store the portion of the software encrypted with the second key value.

3. A system according to Claim 2, wherein the installation server is further configured to generate the first key value and store the first key value as a subsequent second secret value associated with the copy of the software.

4. A system according to Claim 3, wherein the installation server is further configured to retain a copy of an initial second secret value associated with the copy of the software and to selectively provide the initial second secret value to the installation client.

5. A system according to Claim 3, wherein the installation server is configured to maintain a copy of an original second secret value associated with a first key value utilized to encrypt an initial copy of the software and wherein the installation server is configured to control the number of installations allowed for the copy of the software based on a maximum number of installations and a maximum number of times that the original second secret value may be sent to the installation client.

6. A system according Claim 5, wherein the installation server is configured to track the number of times that the copy of the software has been installed and the number of times that the original second secret value is sent to the installation client and wherein the installation server is further configured to reject a request for installation of the copy of the software if the installation results in at least one of the number of times that the copy of the software has been installed exceeding the maximum number of software installations and the number of times that the original second secret value is sent to the installation client exceeds the maximum number of times that the original second secret value may be sent to the installation client.

7. A system according to Claim 2, wherein the installation client is configured to decrypt the

encrypted portion of the software and encrypt the portion of the software with the second key value without persistently storing the decrypted portion of the software, the second secret value, the first key value or the second key value.

8. A system according to Claim 2, wherein the installation client is further configured to replace the encrypted portion of the software with the portion of the software encrypted with the second key value.

9. A system according to Claim 8, wherein the encrypted portion of the software comprises a plurality of encrypted blocks and wherein the installation client is further configured to sequentially decrypt ones of the plurality of encrypted blocks with the first key value and sequentially encrypt and store the decrypted plurality of encrypted blocks with the second key value, wherein a next of the plurality of encrypted blocks is decrypted after a previous of the plurality of encrypted blocks is encrypted with the second key value and stored.

10. A system according to Claim 1, wherein the installation server is further configured to receive a request for installation of the copy of the software from the installation client and provide the second secret value to the installation client in response to the request for installation of the copy of the software.

11. A system according to Claim 10, wherein the installation server is further configured to determine if the requested installation is authorized and provide

the second secret value to the installation client if the requested installation is authorized.

12. A system according to Claim 1, further comprising a network interconnecting the installation server and the installation client.

13. A system according to Claim 12, wherein the network comprises the Internet.

14. A system according to Claim 1, wherein the installation client is further configured to copy at least the encrypted portion of the software from a read only storage device to a writeable storage device and to store the portion of the software encrypted with the second key value so as to overwrite the encrypted portion of the software stored on the writeable storage device.

15. A method of controlling access to software comprising:

providing a copy of the software, the software being divided into a first encrypted portion and a second unencrypted portion, the second unencrypted portion having access to a first secret value and a software identification associated with the copy of the software and wherein the first encrypted portion is encrypted with a first key value which is based on the first secret value and a second secret value associated with the software identification of the copy of the software;

obtaining the second secret value;

generating the first key value from the obtained second secret value and the first secret value;

decrypting the first encrypted portion of the software utilizing the first key value.

16. A method according to Claim 15, further comprising installing the software on a data processing system utilizing the decrypted first encrypted portion of the software.

17. A method according to Claim 15, further comprising:

generating a second key value from the first key value and the first secret value;

encrypting the decrypted first encrypted portion of the software with the second key value; and

storing the first encrypted portion of the software encrypted with the second key value.

18. A method according to Claim 17, wherein the step of storing the first encrypted portion comprises overwriting a stored copy of the first encrypted portion of the software encrypted with the first key value.

19. A method according to Claim 15, wherein the step of obtaining the second secret value comprises the steps of:

requesting the second secret value from a network server; and

receiving the second secret value from the network server in response ot the request for the second secret value.

20. A method according to Claim 19, wherein the step of requesting the second secret value from the network server comprises transmitting a request for the

second secret value containing the identification of the copy of the software.

21. A method according to Claim 20, further comprising the step of obtaining user information and wherein the request for the second secret value further contains the obtained user information.

22. A method according to Claim 21, wherein the user information comprises at least one of identification of a data processing system on which the software is to be installed and identification of a user associated with the copy of the software.

23. A method according to Claim 19, further comprising the steps of:

determining if the request for the second secret value is for an authorized installation of the copy of the software; and

sending the second secret value only if the request is for an authorized installation of the copy of the software.

24. A method according to Claim 23, wherein the determination of whether the request is for an authorized installation of the software is based on at least one of the identification of the copy of the software, an identification of a user of the software, an identification of a processing system on which the software is to be installed, an authorized number of installations for the copy of the software and a number of previous installations of the copy of the software.

25. A method according to Claim 23, further comprising the step of tracking the number of times that the copy of the software has been installed; and

wherein the determination of whether the request is for an authorized installation comprises the step of determining if the number of times that the copy of the software has been installed exceeds a maximum number of times that the software is authorized for installation.

26. A method according to Claim 17, further comprising the steps of:

generating the first key value based on the first and second secret values at the network server; and

associating the first key value with the identification of the copy of the software as an updated second secret value to be provided in response to a subsequent request for the second secret value.

27. A method according to Claim 26, further comprising the steps of:

copying the first encrypted portion of the software from a read only media to a writeable storage media;

generating a second key value from the first key value and the first secret value;

encrypting the decrypted first encrypted portion of the software with the second key value; and

storing the first encrypted portion of the software encrypted with the second key value on the writeable storage media.

28. A method according to Claim 27, further comprising the steps of:

maintaining a copy of the second secret value as an initial second secret value; and

selectively providing the initial second secret value in response to a request for the second secret value.

29. A method according to Claim 28, wherein the step of obtaining the second secret value comprises the steps of:

requesting the second secret value from a network server; and

receiving the second secret value from the network server in response to the request for the second secret value.

30. A method according to Claim 29, further comprising the steps of:

determining if the request for the second secret value is for an authorized installation of the copy of the software; and

sending the second secret value only if the request is for an authorized installation of the copy of the software.

31. A method according to Claim 30, further comprising the step of tracking the number of times that the copy of the software has been installed; and

wherein the determination of whether the request is for an authorized installation comprises the step of determining if the number of times that the copy of the software has been installed exceeds a maximum number of times that the software is authorized for installation.

32. A method according to Claim 31, further comprising the steps of:

determining if the request for installation is a request to resynchronize secret values utilized to generate the first key value; and

providing the initial second secret value if the request for installation is a request to resynchronize secret values.

33. A method according to Claim 32, further comprising the step of tracking the number of times that the initial second secret value has been provided; and

wherein the determination of whether the request is for an authorized installation further comprises the step of determining if the number of times that the second secret value has been provided exceeds a maximum number of times that the second secret value is authorized to be provided.

34. A method according to Claim 15, further comprising the step of:

encrypting the first encrypted portion of the software as a plurality of encrypted blocks;

wherein the step of decrypting the first encrypted portion of the software comprises decrypting an encrypted block of the plurality of encrypted blocks with the first key value;

wherein the step of encrypting the decrypted first encrypted portion of the software comprises encrypting the decrypted block with the second key value;

wherein the step of storing the first encrypted portion of the software encrypted with the second key value comprises storing the block encrypted with the second key value; and

wherein the block of the plurality of encrypted blocks is decrypted, encrypted and stored before a next

block of the plurality of blocks is decrypted, encrypted and stored.

35. A method of controlling software installations, comprising:

associating a software identification and first and second secret values with a copy of the software;

receiving a request for installation of the software on a data processing system, wherein the request identifies the software identification of the copy of the software;

determining the second secret value associated with the software identification;

determining if the installation of the copy of the software to be installed is authorized; and

sending the second secret value to the data processing system if the installation of the copy of the software to be installed is authorized.

36. A method according to Claim 35, wherein the determination of whether the installation of the copy of the software is authorized is based on at least one of the identification of the copy of the software, an identification of a user of the software, an identification of a processing system on which the software is to be installed, an authorized number of installations for the copy of the software and a number of previous installations of the copy of the software.

37. A method according to Claim 35, further comprising the steps of:

generating a first key value from the first and second secret values associated with the copy of the software;

associating the first key value with the software identification of the copy of the software as an updated first secret value.

38. A method according to Claim 37, wherein the step of associating the first key value with the software identification of the copy of the software as an updated first secret value comprises the step of replacing the first secret value associated with the software identification of the copy of the software with the first key value.

39. A system for controlling access to software comprising:

means for providing a copy of the software, the software being divided into a first encrypted portion and a second unencrypted portion, the second unencrypted portion having access to a first secret value and a software identification associated with the copy of the software and wherein the first encrypted portion is encrypted with a first key value which is based on the first secret value and a second secret value associated with the software identification of the copy of the software;

means for obtaining the second secret value;

means for generating the first key value from the obtained second secret value and the first secret value; and

means for decrypting the first encrypted portion of the software utilizing the first key value.

40. A system for controlling software installations, comprising:

means for associating a software identification and first and second secret values with a copy of the software;

means for receiving a request for installation of the software on a data processing system, wherein the request identifies the software identification of the copy of the software;

means for determining the second secret value associated with the software identification;

means for determining if the installation of the copy of the software to be installed is authorized; and

means for sending the second secret value to the data processing system if the installation of the copy of the software to be installed is authorized.

41. A computer program product for controlling access to software comprising:

a computer readable storage media having computer readable program code embodied therein, the computer readable program code comprising:

computer readable program code which provides a copy of the software, the software being divided into a first encrypted portion and a second unencrypted portion, the second unencrypted portion having access to a first secret value and a software identification associated with the copy of the software and wherein the first encrypted portion is encrypted with a first key value which is based on the first secret value and a second secret value associated with the software identification of the copy of the software;

computer readable program code which obtains the second secret value;

computer readable program code which generates the first key value from the obtained second secret value and the first secret value; and

computer readable program code which decrypts the first encrypted portion of the software utilizing the first key value.

42. A computer program product for controlling software installations, comprising:

a computer readable storage media having computer readable program code embodied therein, the computer readable program code comprising:

computer readable program code which associates a software identification and first and second secret values with a copy of the software;

computer readable program code which receives a request for installation of the software on a data processing system, wherein the request identifies the software identification of the copy of the software;

computer readable program code which determines the second secret value associated with the software identification;

computer readable program code which determines if the installation of the copy of the software to be installed is authorized; and

computer readable program code which sends the second secret value to the data processing system if the installation of the copy of the software to be installed is authorized.

43. A computer program product for controlling access to software comprising:

a computer readable storage media having computer readable program code embodied therein, the computer readable program code comprising:

computer readable program code which provides a copy of the software, the software being divided into a first encrypted portion and a second unencrypted

portion, wherein the second encrypted portion is encrypted with a first key value; and

computer readable program code provided in the second unencrypted portion which accesses a first secret value and a software identification associated with the copy of the software, receives a second secret value, generates the first key value from the first and second secret values and decrypts the first encrypted portion.